UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/868,314	06/18/2001	David Michael Jarman	5514	8921

6858 7590 06/28/2005

BREINER & BREINER, L.L.C.
P.O. BOX 19290
ALEXANDRIA, VA 22320-0290

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/868,314	JARMAN, DAVID MICHAEL	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 March 2005* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 3/28/2005, applicant has amended claims 1 and 15. The following claims 1-19 are presented for examination.

1.1 In response to communications filed on 3/28/2005, the amendment to the abstract has been considered and the objection to the abstract has been withdrawn.

2. Applicant's arguments, pages 10-11, filed on 3/28/2005, with respect to the rejection of claims 1-19 have been fully considered but they are not persuasive. Applicant has amended claim 1 to add that the encryption key is altered after each transmission. It is well known in the art that keys can be changed periodically to avoid replay attack from eavesdropper. In addition, maintaining a shared secret without using RSA is also well known. All these features are disclosed in Schneier as well known art.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claim 1 and the intervening claims are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3.1 Claim 1 recites the limitation "one encryption key between the data source and the apparatus is altered after each transmission". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.1 **Claims 1-19** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,084,969 to **Wright et al.** in view of International Patent Publication FR 2681165 to **Augustin**. *(Applicant IDS)* and in view of Bruce **Schneier** "Applied Cryptography", 1996; John Wiley & Sons; Second edition; Pages 178-184.

4.2 **As per claims 1** and **15, Wright et al.** substantially teaches a an apparatus for the transmittal, reception, storage and display of data in an electronic format in which there is

provided a casing that includes a data storage means, a data display means, and a data transmission/reception means including at least one output/input port, and wherein the data transmission/reception means includes means-for decrypting received data and placing it in the data storage means, encrypting and transmitting data from the data storage means and means for storing at least one encryption key, and wherein the apparatus is configured such that one encryption key references addresses in a portion of Read only Memory forming part of the apparatus, and the content of those addresses is used to encrypt/decrypt transmitted/received data, for example (see column 6, line 35 through column 7, line 38). **Wright et al.** discloses using key references addresses in memory so that the content of those addresses is used to encrypt/decrypt transmitted/received data, for example (see column 14, lines 16-55). **Wright et al** discloses public/private key using identifier to retrieve keys from memory in the exemplary embodiment but also suggests sharing secret key (column 14, lines 55-67). **Wright et al.** does not explicitly disclose using ROM to store shared secret keys and the key is altered after each transmission. These features are very well known in the art and they are disclosed in "Applied Cryptography" by Schneier.

Schneier in an analogous art discloses storing keys in ROM is a very clever idea because keys are less subject to be compromised when they are protected in hardware and in addition they can be encrypted to make them more secure. (see page 181). **Schneier** further discloses attaching a control vector with keys to control key usage and to prevent users to get at the keys directly (page 180). **Schneier** discloses sharing key between two parties and updating keys after each transmission (page 180, section 8.6); lifetime of a key should be considered as a security measure because the longer a key is used the greater the loss if the key is compromised (page

183). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Wright et al** to use a ROM memory wherein the apparatus is configured such that one encryption key references addresses in a portion of Read only Memory forming part of the apparatus, and so that the content of those addresses is used to encrypt/decrypt transmitted/received data as taught by **Schneier** to make the key tamper resistant as the key is protected in hardware it is less vulnerable to attack form the outside. It would have been obvious to one of ordinary skill in the art at the time the invention was made to share and update keys between the data source and the apparatus wherein one encryption key is altered between the data source and the apparatus after each transmission as taught by **Schneier** to restrict the key to a short lifetime so that if the key is ever compromised the loss will be less than it will be for a longer validity period. The motivation to do so is given by **Schneier** who teaches storing keys in ROM is a very clever idea because keys are less subject to be compromised when they are protected in hardware (pages and teaches that lifetime of a key should be considered as a security measure because the longer a key is used the greater the loss if the key is compromised (page 183).

Augustin discloses storing keys in ROM and using an index to retrieve key that meets the recitation of key to reference addresses of permanent key stored therein so that keys are not transmitted in the clear and further discloses transmitted a secret key that is altered by a base key after each transmission (see abstract). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Wright et al** to use a ROM memory wherein the apparatus is configured such that one encryption key references addresses in a portion of Read only Memory forming part of the apparatus, and using content of

those addresses to encrypt/decrypt transmitted/received data as taught by **Augustin**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Augustin** to use index to store keys in ROM so that keys cannot be accessed by unauthorized party because some sections of the memory can only be accessed by the apparatus itself; also to provide a different key or index to alter the key after each transmission to avoid replay attack and long term loss if the key is compromised.

As per claim 2, the combined references disclose at least one encryption/decryption key is stored Electronically Erasable Programmable portion of either a Read Only Memory or non volatile Random Access Memory, and may be rewritten by an external key issuing computer as discussed above. (See also **Augustin**, end of page 6 for disclosure of EEPROM). Therefore, claim 2 is rejected on the same rationale as the rejection of claim 1.

As per claims 3-4, Wright et al. discloses the option of choosing key size suitable for design use (column 7, lines 55-65).

As per claims 8, 12, and 13, Wright et al. substantially discloses a method of using apparatus according to claim 1 or 2 for the reception of electronic data from an external data source comprising:

i) entering the apparatus into electronic communication with the data source and sends an identification code to the data source, for example (see column 9, line 10 through column 10);

ii) confirmation by the data source of the identity of the apparatus and thereby determines what encryption key to use in communicating with the apparatus, for example (see column 9, lines line 35 through column 10, line 32);

iii) sending by the apparatus a code to the data source identifying the data to be received by the apparatus, for example (see column 9, lines line 35 through column 10, line 32);

iv) transmission by the data source of the identified data in encrypted form to the apparatus which decrypts that data and places it in the data storage means, for example (see column 13);

v) transmission by the data of a new encryption key to the apparatus, which key overwrites the previous encryption key, for example (see column 14) and vi); breaking the communication between the apparatus and the data source. It is apparent that the communication can terminate after receiving requested data. Claim 12 recites the same inventive concept except for switching the function of the end user. The destination and the source can perform the same function and they can represent the same entity without departing from the spirit and scope of the invention disclosed by **Wright et al** or the same encryption process can be applied with two parties as in the invention disclosed by Augustin.

Claims 5-7 and 9-11 recite the data storage means comprised of non volatile Random Access Memory, in which the at least one output/input port is adapted to connect with a telephone socket via an electromagnetic radiation link, or via telephone network or via Internet, in which the display means includes a display screen and computer hardware and software to enable presentation of the data in graphical and/or textual form. **Wright et al** discloses an apparatus capable of storing in RAM and capable of using the Internet via a phone network or

wireless communication and display capable of showing graphic and text (column 6, lines 35-67 and column 8); therefore, they are rejected on the same rationale as claims 1, 8, and 12.

As per claim 14, Wright et al discloses the limitation of the electronic data is transmitted from the data store to the apparatus, and is saved in the apparatus in decrypted form (column 14, lines 50-55).

As per claim 16, Wright et al discloses the limitation of in which the data store will on interrogation by the apparatus, provide the apparatus with a list of the data stored within the data store (column 14, lines 49-55).

Claims 17-19 recite the same limitation as the previous claims such as 9-11. Therefore, they are rejected on the same rationale.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Carl Colin
Patent Examiner
June 22, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100